

(f) Other egregious security incident (as determined by the DoD Component senior agency official).

(2) Security incidents that do not meet the reporting criteria specified above shall be filed in a retrievable format by the DoD Component and shall be available for inspection or further analysis, review, and potential investigation.

(3) On behalf of the Secretary of Defense, the USD(I) shall notify Congress and the Director, ISOO, regarding specific cases or incidents as required by References (d) and (bk).

(4) The Director of Security, OUSD(I), shall coordinate with the Office of the DNI (ODNI) National Counterintelligence Executive (NCIX) as needed to ensure notifications required by Intelligence Community Directive 701 (Reference (bl)) are made.

#### 4. CLASSIFICATION OF REPORTS

a. Security incident reports shall be classified according to the content of the report and at the level prescribed by the applicable program security classification guides. At a minimum, reports shall be designated FOUO and marked as required by Volume 4 of this Manual, in order to provide appropriate protection for information regarding personnel involved and information that could facilitate unauthorized access to classified information. If the lost or compromised information is beyond the jurisdiction of the U.S. Government and cannot be recovered (e.g., media leak, public website posting, or loss in a foreign country), the report and location of the compromise (e.g., geographic location of unrecoverable equipment) shall be classified commensurate with the classification level of the compromised material to prevent further unauthorized disclosure.

b. If an FOUO report is to be disseminated outside the Department of Defense (e.g., to another Federal agency), the face of the document shall bear an expanded marking, as specified in Enclosure 3 of Volume 4 of this Manual, stating that the information may be exempt from mandatory disclosure pursuant to section 552 of title 5, U.S.C. (also known as “The Freedom of Information Act” and hereinafter referred to as “FOIA” (Reference (bm))).

c. Reports, whether classified or unclassified, disclosing technical data shall be marked with the appropriate distribution statement as described in DoDD 5230.24 (Reference (bn)) or associated with the information involved in the incident.

5. SPECIAL CIRCUMSTANCES. Certain types of classified information or specific circumstances require unique handling or consideration of additional reporting requirements as specified in paragraphs 5.a through 5.o.

a. Security Incidents Involving Deliberate Compromise, a Foreign Intelligence Service or a Terrorist Organization. Any incident in which deliberate compromise of classified information or involvement of a foreign intelligence service, international terrorist group, or organization is

suspected shall be reported immediately to the cognizant Defense CI component, in accordance with DoDD 5240.06 (Reference (bo)). Security officials shall not initiate or continue an inquiry or investigation of the incident unless it is fully coordinated with the cognizant Defense CI component.

b. Security Incidents Involving Apparent Violations of Criminal Law. Any incident in which an apparent violation of criminal law is suspected, but which is reasonably not believed to be espionage or involving matters described in paragraph 5.a of this section, shall be reported immediately to the local DCIO. If that organization accepts jurisdiction and initiates action, coordinate with them prior to taking any further action on the security inquiry or investigation so as not to jeopardize the integrity of either investigation.

c. Security Incidents Involving COMSEC or Cryptologic Information. Actual or potential compromises involving cryptographic information shall be handled according to NSTISSI 4003 (Reference (bp)).

d. Security Incidents Involving SCI. Actual or potential compromises involving SCI shall be reported to the activity SSO and handled in accordance with References (i) and (bl).

(1) Incidents involving SCI that meet the criteria in paragraph 3.f of this enclosure shall also be reported to the Director of Security, OUSD(I).

(2) If a DoD Component believes a disclosure may contain classified SCI information under the control of an(other) Intelligence Community agency, the DoD Component shall notify NCIX. NCIX shall coordinate notification to the affected agency.

e. Security Incidents Involving RD and/or FRD. In accordance with the provisions of section 3161 of Public Law 105-261 (Reference (bq)), and its implementing plan, the Secretary of Energy must report to Congress inadvertent disclosure of RD or FRD occurring pursuant to automatic declassification processes. Components shall notify the Department of Energy as necessary and provide a copy of the notification to the Deputy Assistant Secretary of Defense for Nuclear Matters and the Director of Security, OUSD(I).

f. Security Incidents Involving IT. Actual or potential compromises of classified information involving IT, automated information systems, or computer systems, terminals, or equipment shall be reported, in accordance with Reference (bf), through appropriate channels by the IA manager (IAM) to the activity security manager. Inquiries into and resolution of incidents involving compromise of classified information resident on computers or in IT systems require coordination with and assistance from the local IA officials, but prompt resolution remains the responsibility of the activity security manager. See Enclosure 7 for additional guidance on handling of classified data spills.

g. Security Incidents Involving FGI or NATO Information. Actual or potential compromises involving FGI or NATO information shall also be reported promptly by the DoD Component senior agency official to the USD(P), who serves as the DSA. The Director, International Security Programs, Defense Technology Security Administration, OUSD(P), shall be

responsible, on behalf of the DSA, for notifying and coordinating with NATO or the foreign government, as appropriate.

h. Security Incidents Involving Classified U.S. Information Provided to Foreign Governments. Actual or potential compromises of U.S. classified information held by foreign governments shall be reported to the originating DoD Component, the OCA, the Director of Security, OUSD(I), and the Director, International Security Programs, Defense Technology Security Administration, OUSD(P).

i. Security Incidents Involving SAPs. Actual or potential compromises involving DoD SAPs, or results of inquiries and/or investigations that indicate that weaknesses or vulnerabilities in established SAP policy and/or procedures contributed to an actual or potential compromise, shall be reported by the DoD Component SAP program office to the DoD SAP Central Office, which shall report to the Director of Security, OUSD(I).

j. Security Incidents Involving Improper Transfer of Classified Information. Any activity that receives classified information that has been improperly handled, addressed, packaged, transmitted, or transported shall make a determination as to whether the information has been subjected to compromise. If the activity determines that the classified information has been subjected to compromise, the receiving activity shall immediately notify the sending activity, which shall be responsible for initiating an inquiry or investigation, as appropriate. The receiving activity shall share information generated regarding the incident with the sending activity. The sending activity is responsible for required notifications (e.g., to the OCA). Classified information shall be considered as having been subjected to compromise if it has been handled through foreign postal systems, its shipping container has been damaged to an extent that the contents are exposed, or it has been transmitted (e.g., telephone, facsimile, message, e-mail, computer or data links) over communications circuits that are not approved for transmission of classified information. If the receiving activity determines that classified information was not in fact compromised, but was nevertheless improperly prepared or transferred, the receiving activity shall report the discrepancy to the sending activity.

k. Security Incidents Involving On-Site Contractors. Security incidents, including any inquiries or investigations required, involving on-site contractors shall be handled in accordance with paragraph C1.1.9 of Reference (ba). As specified by paragraph C1.1.9 of Reference (ba) and paragraph 6-105c of Reference (x), host activity security rules and procedures apply. Disciplinary action and sanctions are the responsibility of the contractor's company unless specific contract provisions address such actions. Security managers shall furnish the results of inquiries to the company, with a copy to Defense Security Service, in order to facilitate such action. Specified U.S. Government officials retain the ability, when appropriate and in accordance with the authorities and requirements of Reference (ba), to deny access to classified information, to revoke or suspend security clearances, and to take certain other administrative actions, such as to deny an individual continued access to the facility.

l. Security Incidents Involving Critical Program Information (CPI). Upon learning that classified CPI or CPI related to classified contracts may have been or was actually compromised, security officials shall inform the program manager of record and the cognizant Defense CI

component pursuant to DoDD O-5240.02 (Reference (br)). The specific CPI involved in the incident should be identified in inquiry and investigation reports. Classify reports as required by the applicable program security classification guide(s).

m. Security Incidents Involving ACCM-Protected Information. Security officials shall refer to section 18 of Enclosure 2 of this Volume for additional guidance on security incidents involving ACCM-protected information as well as safeguarding and handling of ACCM-protected information.

n. Absence Without Authorization. When an individual who has had access to classified information is absent without authorization, the head of the activity or security manager shall determine if there are indications of activities, behavior, or associations that could indicate classified information may be at risk. If so, the supporting Defense CI component shall be notified in accordance with Reference (br). The scope and depth of the inquiry shall depend on the length of absence and the sensitivity of the classified information involved. Missing personnel authorized SCI access shall be reported in accordance with Reference (i).

o. Coordination with Legal Counsel and the Department of Justice (DoJ). Whenever formal action, beyond adjudication of a finding of a security violation and assignment of reprimand or disciplinary action at the activity level is contemplated against any person believed responsible for the unauthorized disclosure of classified information, DoD Component officials shall coordinate with servicing legal counsel. Whenever a criminal violation appears to have occurred and a criminal prosecution is contemplated, Component officials shall use established procedures and channels to ensure coordination with the legal counsel of the DoD Component or Federal agency where the individual is assigned or employed and the DoJ.

## 6. SECURITY INQUIRIES AND INVESTIGATIONS

a. Requirement. All known or suspected instances of unauthorized disclosure of classified information shall be promptly addressed by the cognizant DoD Component to decide the nature and circumstances of the disclosure and the extent of damage to national security, and appropriate corrective action shall be taken. See Appendix 1 to this enclosure for a sample, optional format for use in documenting actions. Reports of inquiries and investigations, at a minimum, shall be designated and marked as FOUO.

b. Coordination with Criminal Investigative Organization or Defense CI Component. When information suggestive of a criminal or CI nature is discovered, all actions associated with the inquiry or investigation shall cease pending coordination with the cognizant DCIO or Defense CI component. If the DCIO or Defense CI component accepts jurisdiction, the inquiry or investigation shall not be resumed without agreement of the cognizant criminal investigative organization or CI component. All relevant information shall be released with an annotation in the report that the matter was referred to the specific DCIO or Defense CI component. Notify the OCA, originator, and others as appropriate, after coordination with the DCIO or Defense CI component. If the DCIO or Defense CI component declines jurisdiction, the security inquiry or investigation shall continue. Annotate the report appropriately and include the identity of the